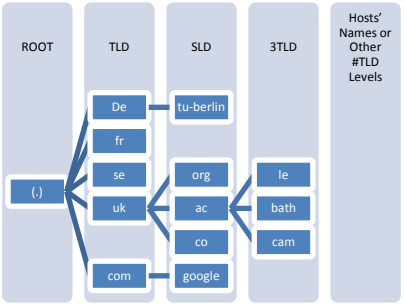
University of Leicester

Marwan M Radwan, mmmr1@le.ac.uk
Supervisor: Prof. Dr. Reiko Heckel
College of Science and Engineering,
Computer Science Department.

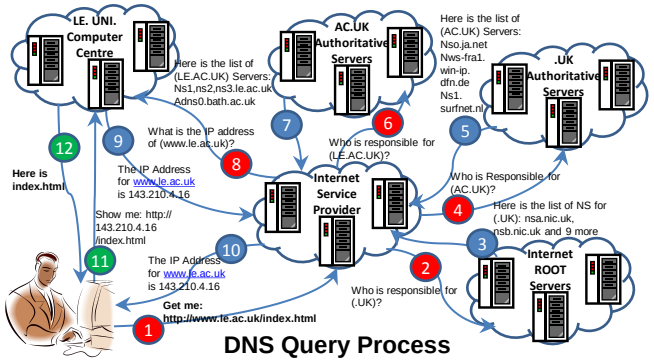
Sniffing Out and Fixing Fishy Domain Name Configurations

The DNS is a critical component of the Internet. It provides information essential to the operation of every Internet service and application. Operational decisions and deployment choices need to be soundly made in order to create a balancing act between the complexity, overhead, security and resilience of the DNS system.

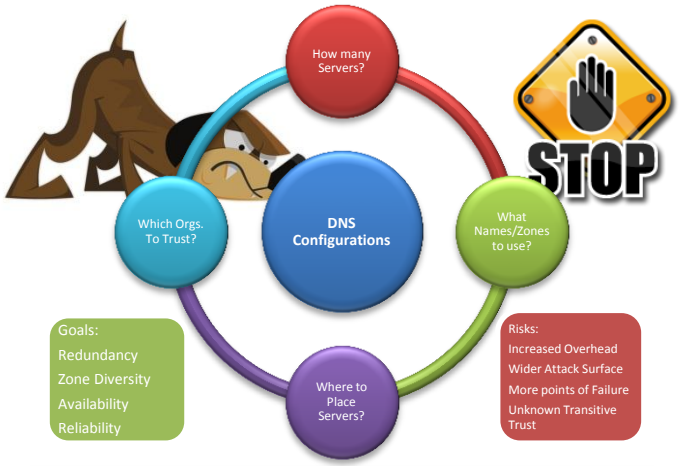


DNS relies on a *delegation*: resolution of a name to its IP address requires resolving the names of the servers responsible for that name, which in turn, depend on their name resolutions, creating complex interdependencies among DNS zones and servers.

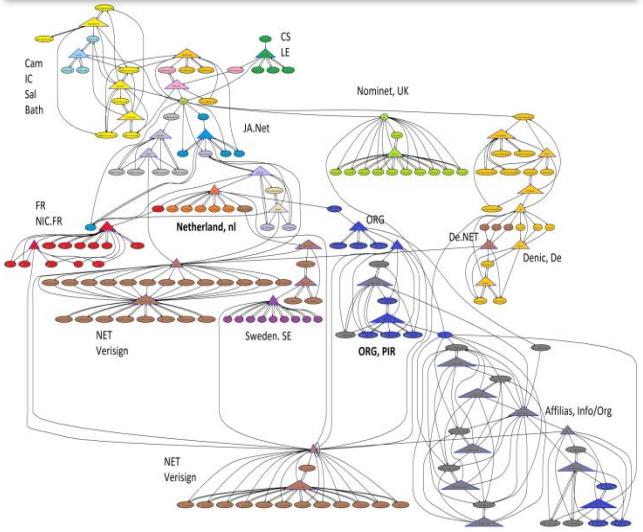
http://www.le.ac.uk → DNS → 143.210.4.16



DNS Query Process



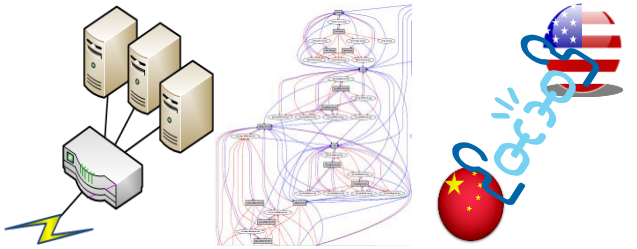
Improve availability, resilience and security without compromising the robustness and redundancy achieved by the diversity and distribution of DNS servers.



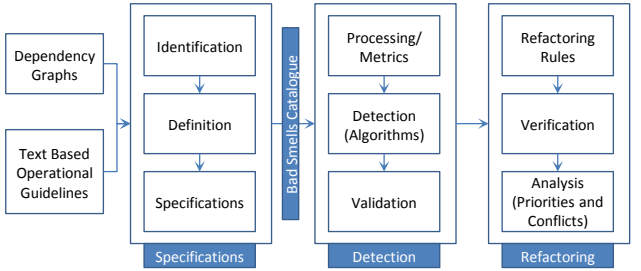
Bad Smells and Refactoring

We utilize *dependency graphs* to detect vulnerabilities and propose graph-based *refactoring rules* to repair them.

False/Diminished Redundancy	Large Attack Surface	"Corrupted!" Parent/Peer
Microsoft.com (2001)	.sd TLD (208 nodes)	US/CN (Politics/trust)



DNS Operational Bad Smells Refactoring Framework



References:
1- E. Osterweil, et. al ."Operational implications of the DNS control plane"
2. V. Ram. et. al. "Perils of transitive trust in the domain name system,"
3. C. Deccio "Measuring availability in the domain name system"
4. V. Pappas, Z. Xu, S. Lu, D. Massey, A. Terzis, and L. Zhang: "Impact of configuration errors on DNS robustness", 2009